REMARKS

Claims 43-83 remain in this application, with Claim 1-42 canceled and new Claims 43-83 added. Applicants respectfully request reconsideration and review of the application in view of the foregoing amendments and following remarks.

Before addressing the merits of the rejections based on prior art, Applicants provide the following brief description of the patent application. The invention provides a form of data encryption/decryption in which the encrypted information can be decrypted only at a specified location. The location information is used to generate the keys to encrypt and decrypt the information, referred to herein as a geolocking key. If someone attempts to decrypt the data at another location, the encryption and decryption keys will not match, and the decryption process fails. The device performing the decryption determines its location using some sort of location sensor, such as a GPS receiver or other satellite or radio frequency positioning system.

More specifically, the patent application describes the use of a location identity attribute that defines a specific geographic region. The location identity attribute comprises a location value that identifies a unique location within the geographic region and a proximity value that identifies an area that encompasses the unique location. A relative location parameter is derived from the location identity attribute that maps all coordinates within the specific geographic region into a common value without identifying a location of the specific geographic region. The digital information is encrypted using a key based on the location identity attribute and the relative location parameter. The appliance that receives the encrypted digital information generates a matching key to decrypt the digital information based on its knowledge of the physical location of the appliance and the relative location parameter received from the sender. Notably, the decrypting key is not communicated to the receiving appliance—to the contrary, it is generated at the receiving end. If the appliance location is not within the proximate area of the location identity attribute, the appliance will be unable to generate

a matching key to decrypt the digital information. As a result, the digital information cannot be decrypted and the security of the information is maintained.

The claims of the present application address both ends of the information communication process, i.e., encrypting (sending) end and decrypting (receiving) end. Independent Claim 43 addresses both the encryption of information at the sending end and the decryption at the receiving end. Independent Claim 62 addresses only the encryption of information at the sending end. Independent Claim 74 addresses only the decryption of the information at the receiving end.

The Examiner rejected Claims 1-8, 11, 14-19, 21-29, 32-39, and 41-42 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Schipper et al. The Examiner rejected Claims 9-10, 12-13, 20, 30-31, and 40 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Schipper et al., and further in view of Shimada. In view of Applicants' cancellation of these claims, these grounds of rejection are moot. Moreover, the cited references are deemed inapplicable to the claims as now presented.

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated.

As discussed by Applicants previously, there are very significant differences between Murphy and the present invention. First of all, Murphy does not disclose the

encryption of data signals. To the contrary, the reference is directed solely to the decryption of encrypted signals. In fact, Murphy includes no discussion of the source of the encrypted signals other than that they are transmitted to the licensed sites by one or more satellites. See col. 7, lns. 23-26. Murphy therefore has no applicability whatsoever to independent Claims 43 or 62, which each address the encryption of information at the sending end of a communication system. The Examiner fails to consider this deficiency of Murphy in the present Office Action, and otherwise provides no explanation of how the proposed combination of references makes up for this deficiency.

Second, Murphy does not use location information to generate a decryption key, and does not encrypt or decrypt digital information using a geolocking key based on a location identity attribute. In fact, Murphy does not generate either an encryption key or decryption key, but rather simply activates the decryption chip that is included on the decryption module. The Examiner has acknowledged these deficiencies of Murphy in the present Office Action, and proposes the combination with Schipper to make up for these deficiencies.

The Examiner further asserts that Murphy discloses the use of a "shape parameter (column 7 lines 5067), in the form of a circle with a varying diameter." Even though the term "shape parameter" no longer appears in the claims, Applicants respectfully disagree with the Examiner's characterization. In Murphy, the diameter value is used to determine whether the user is within a predetermined range of the licensed site location. Notably, Murphy does not use the diameter value as an input to generate an encryption or decryption key, nor does Murphy communicate the diameter value to the recipient along with the encrypted data, nor. The disclosure of the diameter value by Murphy appears to have nothing in common with the "relative location parameter" defined in the claims.

Schipper discloses a method of communicating between mobile stations using present and past location information to vary an encryption key. The mobile stations

each have a satellite positioning system (SATPS) receiver and antenna that receive signals from a plurality of navigation satellites. The SATPS receiver generates pseudorange measurements from that station to each navigation satellite in view, and produces location information based on a plurality of pseudorange measurements. Schipper periodically communicates pseudorange correction (PRC) values from a base station to the mobile stations, which in turn use these PRC values to correct their own location determinations. By design, Schipper purposefully eliminates location from the PRC values by calculating it as the differential between the known base station location and the SATPS pseudorange measurements. Each mobile station also uses the PRC values as a parameter to determine an encryption key used to encrypt messages transmitted back to the base station and/or to other mobile stations.

There are significant differences between Schipper and the present invention. First, there is no indication in Schipper that the encryption key would be generated using a "location identity attribute that identifies a specific geographic region." As described above, the PRC does not identify any specific geographic region. Second, Schipper does not disclose any generation of a decryption key used for decrypting received messages. Instead, the PRC is used to generate an encryption key to be used in encrypting messages that are communicated back to the base station and/or to other mobile stations. Schipper does not disclose how a corresponding recipient of the encrypted information would generate a decryption key to recover the information from the encrypted message. Even if the generation of the encryption key were construed as analogous to the generation of a decryption key, Schipper does not use any current location information as an input to the key generation process. More specifically, Schipper does not generate an encryption key using any information corresponding to the location of the intended recipient of the encrypted information, and does not generate a decryption key using "current location" information.

Accordingly, a combination of the references would fail to suggest or disclose several aspects of the invention defined in the foregoing claims. First, neither reference

suggests or discloses the use of a "location identity attribute" and a "relative location parameter" to generate an encryption key. Second, neither reference suggests or discloses the use of "current location" of a recipient to generate a decryption key. Third, neither reference suggests or discloses the derivation of a "relative location parameter" that maps all coordinates within a specific geographic region into a common value without identifying a location of the specific geographic region. The proposed combination of references therefore fail to establish a *prima facie* case of obviousness.

Shimada discloses a data processing method in which access to information is controlled using a password and location attribute data. A data file includes fields for the attachment of attributes defining a password and location. When it is desired to access the data file, a data processing system compares the attached password to one inputted by a user, and also compares the attached location data to a current location determined by a location determining system (e.g., GPS). If the password is correct and the location matches, then access to the data file is permitted.

The Examiner repeats the erroneous conclusion that Shimada discloses a system in which a "shape file" is included with the file that contains the digital information. By "shape file," the Examiner appears to refer to the location data contained in the data-attribute table 10 (see Shimada, Fig. 2). Even though the term "shape parameter" no longer appears in the claims, Applicants disagree with the Examiner's characterization. The location data of Shimada provides a descriptor that clearly identifies the location. A fundamental advantage of the "relative location parameter" of the present invention is that it can be communicated in the clear to the recipient without jeopardizing the security of the encrypted data, i.e., without disclosing the location identity attribute used to generate the encryption key. Shimada is therefore of no applicability to the present invention.

In view of the foregoing, Applicants respectfully submit that Claims 43-85 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing

this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

The Commissioner is authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,

Date: October 5, 2005

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000